Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A copy protection method for digital media, the method comprising the steps of:

(a) encrypting an original media data set with a media key having a symmetric algorithm and encrypting said media key with ~~each~~ public key of compliant devices;

(b) delivering said encrypted media data set and said encrypted media key to a compliant playing device, wherein said original media data set includes an owner watermark containing an owner identification and owner copy-control information for the media data set;

(c) decrypting said delivered media key with a private key of said playing device;

(d) decrypting said delivered media data set with said decrypted media key;

(e) adding a player watermark to said decrypted media data set if said decrypted data set is not marked with at least "free copy", said player watermark containing a player identification of said playing device and player copy-control information, wherein said player copy-control information is derived from said owner copy-control information;

(f) encrypting said watermark-added media data set with said decrypted media key and encrypting said decrypted media key with said ~~each~~ public key of compliant devices; and

(g) passing said media data set and media key encrypted in the step (f) to ~~a~~ an external compliant ~~recording~~ device.

2. (Currently Amended) The method of claim 1, wherein said ~~each~~ public key corresponds to an asymmetric algorithm.

3-4. Canceled

5. (Currently Amended) A copy protection method for digital media, the method comprising the steps of:

(a) encrypting an original media data set with a media key having a symmetric algorithm and encrypting said media key with ~~each~~ public key of compliant devices;

(b) delivering said encrypted media data set and said encrypted media key to a compliant playing device, wherein said original media data set includes an owner watermark containing an owner identification and owner copy-control information for the media data set, wherein the encrypted media data set can be delivered if the owner copy-control information does not indicate "copy-protected";

(c) decrypting said delivered media key with a private key of said ~~playing~~ compliant device;

(d) decrypting said delivered media data set with said decrypted media key;

(e) adding a ~~player~~ device watermark to said decrypted media data set if said decrypted data set is not marked with at least "free copy", said ~~player~~ device watermark containing a ~~player~~ device identification of said ~~playing~~ compliant device and ~~player~~ copy-control information, wherein said copy-control information is derived from said owner copy-control information;

(f) performing a compliance test through an authentication handshake process between said ~~playing~~ compliant device and ~~a displaying~~ external device; and

(g) transferring said watermark-added media data set to said ~~displaying~~ external device only if said ~~displaying~~ external device passes said test.

6. (Currently Amended) The method of claim 5, wherein said ~~each~~ public key corresponds to an asymmetric algorithm.

7-8. Canceled

9. (Currently Amended) The method of claim 5, wherein said ~~player~~ copy-control information is set to "for display only".

10. (New) The method of claim 5, wherein the step (g) transfers said watermark-added media data set to said external device after encrypting said watermark-added media data set.

11. (New) A copy protection method for digital media, the method comprising:

(a) receiving an encrypted media data set, a control information, and an encrypted media key, wherein the encrypted media data is generated by an original media

data set with a media key and the encrypted media key is generated by encrypting said media key with a public key of compliant device, wherein the control information includes owner identification of media data set and a copy control information to indicate whether a copy of the media data set permitted;

(b) decrypting said received media key with a private key of said compliant device, and decrypting said received media data set with said decrypted media key;

(c) adding a device information to the media data set to indicate an origin of the media data set, said device information including a device identification and copy-control information, wherein said copy-control information is derived from said owner copy-control information; and

(d) outputting said media data set to which the device information is added, to an external device.

12. (New) The method of claim 11, wherein the step (c) further includes encrypting said media data set to which the device information is added, with a key.

13. (New) The method of claim 12, further comprising:

performing an authentication process between said compliant device and the external device prior to outputting said media data set to which the device information is added, wherein the step (d) outputs the said media data set to which the device information is added only if the authentication is successful.